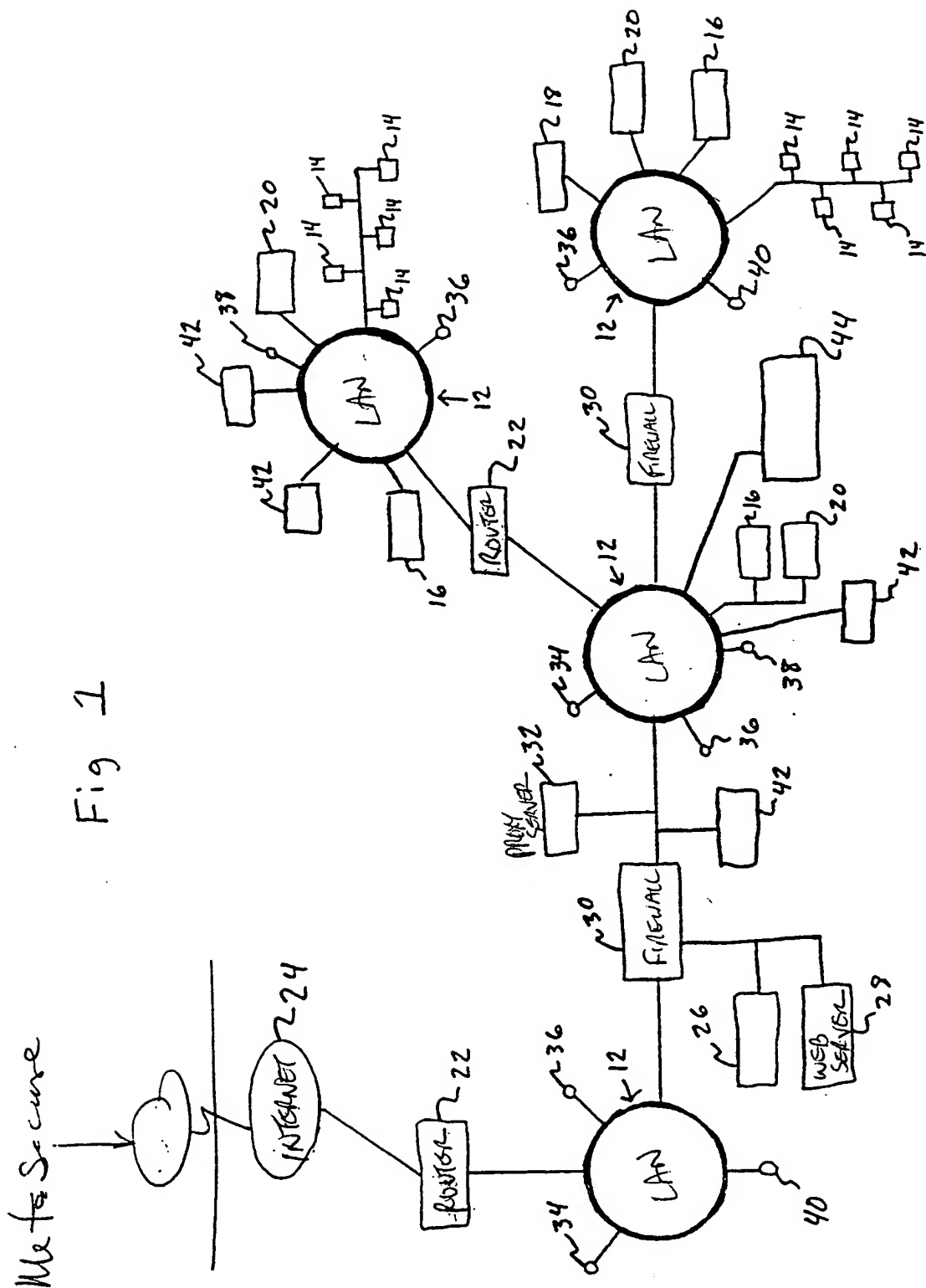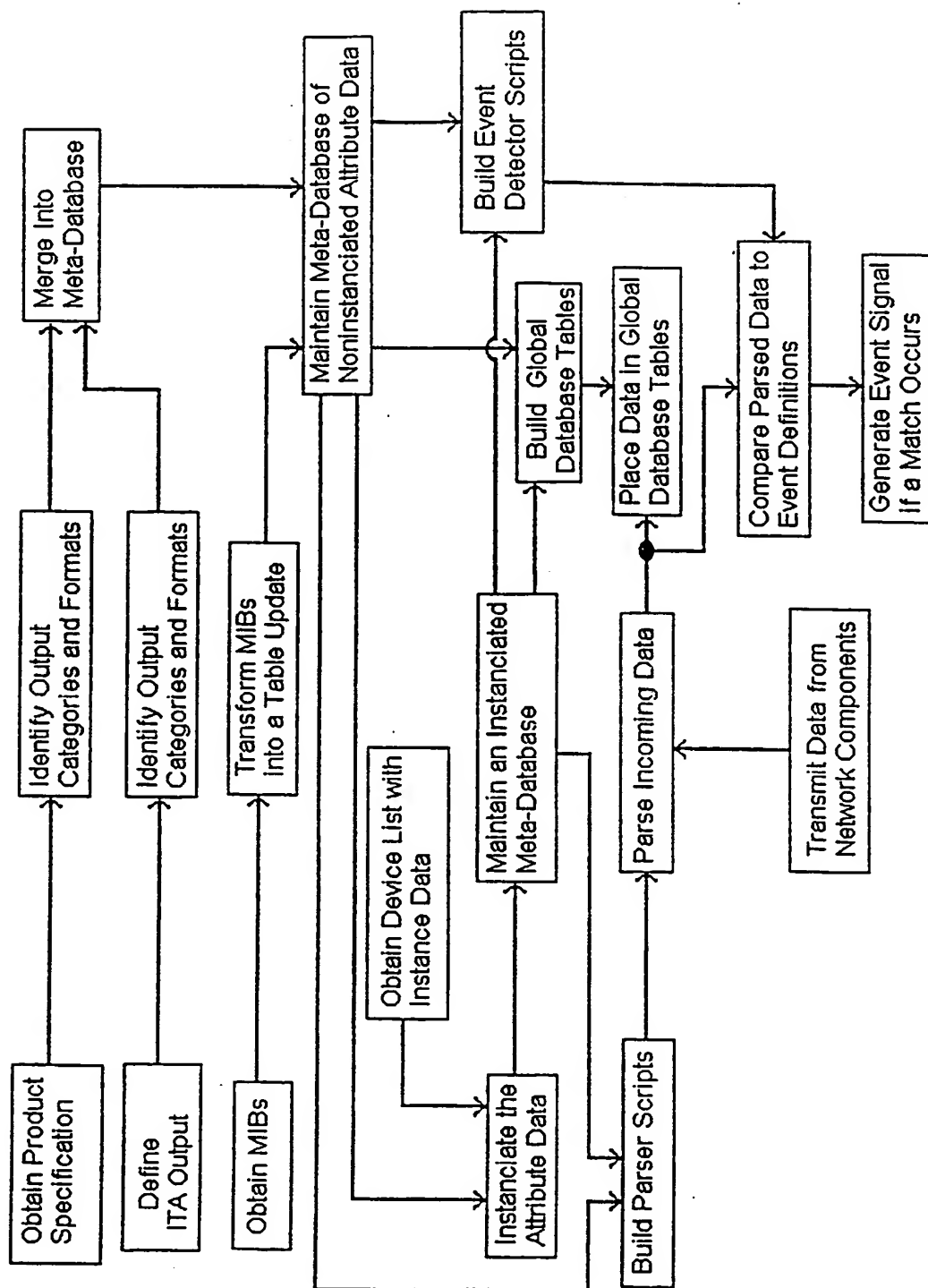Fig 1

Figure 2

Figure 3

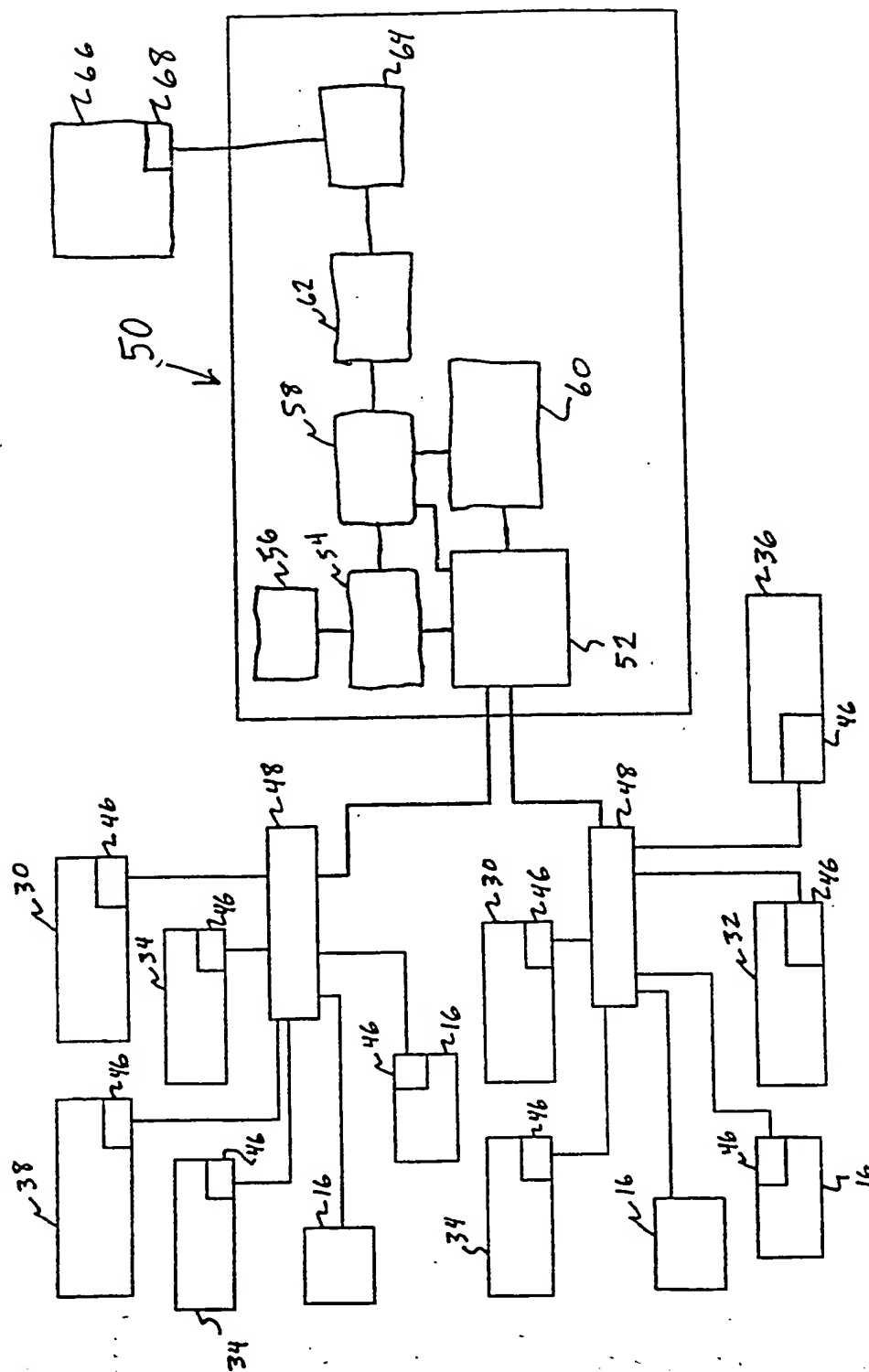Figure 4
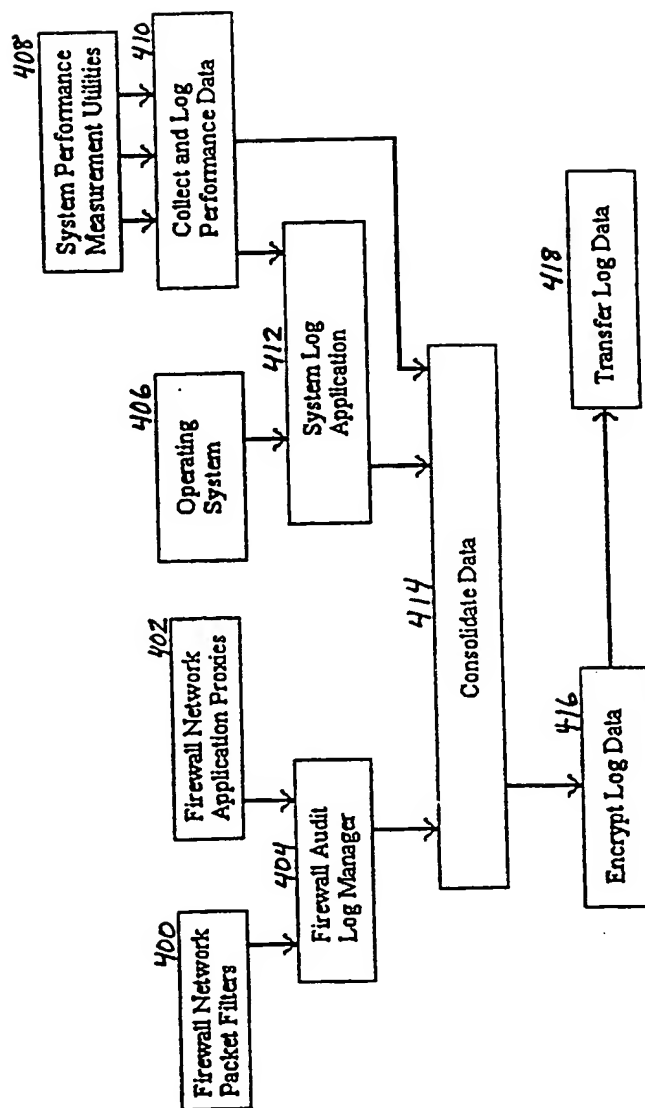
Figure 5
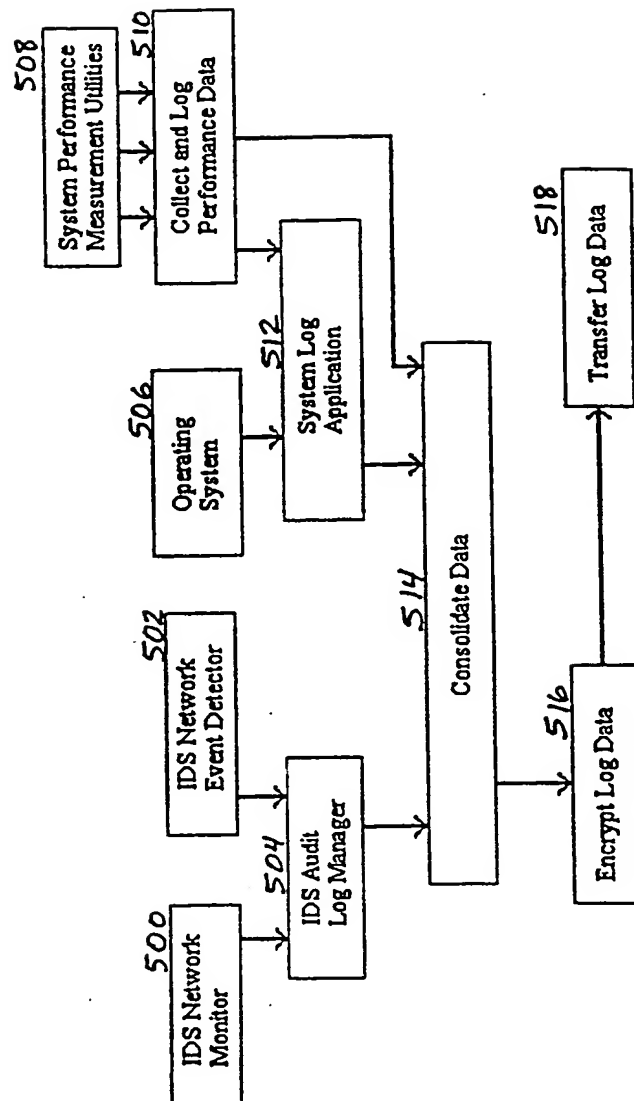
Figure 6

Transaction Table 700

xaction id	name	description	stream id	system type id	conditional
X200164	Network Transaction	A record of a network transaction through a CyberGuard firewall	R100204	T100001	($Action == "T")
X317109	CPU Utilization	A record of CPU percent idle, percent system, percent I/O, and percent user	R113203	T100001	TRUE

System Type Table 702

system type id	make	model	title	load	version	revision	patch
T100001	CyberGuard Corp	3412-02	CyberGuard Firewall For UNIX	CyberGuard	2	2.3	11

Stream Table 704

stream id	stream type	stream path	end of record	end of field
R100204	DELIMITED FLAT FILE	/var/audit_log/old/NetguardID	NEWLINE	SPACE
R113203	FIXED FORM FLAT FILE	/store/compressed/intst.log	NEWLINE	N_A

Figure 7

Element Table 706

section id	element id	name	description	legal value	data unit	refresh period	sample period	period unit	aggregate
X200184	E312073	Date	Date of network transaction	DATE_ISO	N A	ASYNC	SYNC	N A	N A
X200184	E312074	Time	Time of network transaction	TIME_24	N A	ASYNC	SYNC	N A	N A
X200184	E312075	Action	Transaction Type	CHAR	N A	ASYNC	SYNC	N A	N A
X200184	E312076	Source IP	Name of source firewall network interface	ALPHANUMERIC	N A	ASYNC	SYNC	N A	N A
X200184	E312077	Destination IF	Name of destination firewall network interface	ALPHANUMERIC	N A	ASYNC	SYNC	N A	N A
X200184	E312078	Source Address	Source IP address of packet	IP_4	N A	ASYNC	SYNC	N A	N A
X200184	E312079	Destination Address	Destination IP address of packet	IP_4	N A	ASYNC	SYNC	N A	N A
X200184	E312080	Protocol	IP protocol of packet	IP_PROTOCOL	N A	ASYNC	SYNC	N A	N A
X200184	E312081	Source Port	Source port number / service name of packet or ICMP type	ALPHANUMERIC	N A	ASYNC	SYNC	N A	N A
X200184	E312082	Destination Port	Destination port number / service name of packet or ICMP type	ALPHANUMERIC	N A	ASYNC	SYNC	N A	N A
X200184	E312083	Packets_Sent	Number of packets passed from source to destination	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N A	N A
X200184	E312084	Packets_Received	Number of packets passed from destination to source	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N A	N A
X200184	E312085	Bytes_Sent	Number of bytes passed from source to destination	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N A	N A
X200184	E312086	Bytes_Received	Number of bytes passed from destination to source	UNSIGNED_INT_32	COUNT	ASYNC	SYNC	N A	N A
X317189	E444120	Date	Date of measurement	DATE_ISO	N A	ASYNC	SYNC	N A	N A
X317189	E444121	Time	Time of measurement	TIME_24	N A	ASYNC	SYNC	N A	N A
X317189	E444122	CPU Idle	Percent CPU Idle	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE
X317189	E444123	System Percentile	Percent of CPU used for system tasks	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE
X317189	E444124	I/O Percentile	Percent of CPU used for I/O tasks	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE
X317189	E444125	User Percentile	Percent of CPU used for user tasks	UNSIGNED_INT_16	PERCENT	1	10	MINUTE	AVERAGE

Delimited Flat File Table 708

element id	encoding	record num	field num	subfield delim	subfield num	start in field	end in field
E312073	ASCII_7_BIT		ALL	NONE	1	0	0
E312074	ASCII_7_BIT		ALL	NONE	2	0	-1
E312075	ASCII_7_BIT		ALL	NONE	3	0	0
E312076	ASCII_7_BIT		ALL	/	4	0	0
E312077	ASCII_7_BIT		ALL	/	4	1	0
E312078	ASCII_7_BIT		ALL	NONE	5	2	0
E312079	ASCII_7_BIT		ALL	NONE	6	0	0
E312080	ASCII_7_BIT		ALL	NONE	8	0	0
E312081	ASCII_7_BIT		ALL	NONE	9	0	0
E312082	ASCII_7_BIT		ALL	NONE	10	0	0
E312083	ASCII_7_BIT		ALL	NONE	11	0	0
E312084	ASCII_7_BIT		ALL	NONE	12	0	0
E312085	ASCII_7_BIT		ALL	NONE	13	0	0
E312086	ASCII_7_BIT		ALL				

Fixed Form Flat File Table 710

element id	encoding	record num	start in record	end in record
E444120	ASCII_7_BIT	ALL	1	10
E444121	ASCII_7_BIT	ALL	12	19
E444122	ASCII_7_BIT	ALL	21	23
E444123	ASCII_7_BIT	ALL	24	26
E444124	ASCII_7_BIT	ALL	27	29
E444125	ASCII_7_BIT	ALL	30	32

Figure 8

Transaction Table 700
- xaction Id
- name
- description
- stream Id
- system type Id
- conditional

System Type Table 702
- system type Id
- function
- make
- model
- title
- load
- version
- revision
- patch

Stream Table 704
- stream Id
- stream type
- stream path
- end of record
- end of field

Element Table 706
- xaction Id
- element Id
- name
- description
- legal value
- data unit
- refresh period
- sample period
- period unit
- aggregate

<— Input Form Table —>

Delimited Flat File Tabl 708
- element Id
- encoding
- record num
- field num
- subfield delim
- subfield num
- start in field
- end in field

Fixed Form Flat File Table 710
- element Id
- encoding
- record num
- start in record
- end in record

System Table 712
- system Id
- host name
- domain name
- description
- default route
- serial number
- license key
- organization
- location
- contact

Interface Table 714
- system Id
- If name
- If host name
- If IP address
- If network mask
- If side
- If type
- If speed

system Id xaction Id Data Table 716
- element 1
- element 2
- element 3
- ...
- element n

System Id S0214 → S0214_X200154 → S0214_X317189   718 / 720

S0214_X200154
- Date
- Time
- Action
- Source_IF
- Destination_IF
- Source_Address
- Destination_Address
- Protocol
- Source_Port
- Destination_Port
- Packets_Sent
- Packets_Received
- Bytes_Sent
- Bytes_Received

S0214_X317189 720
- Date
- Time
- CPU Idle
- System Percentile
- I/O Percentile
- User Percentile

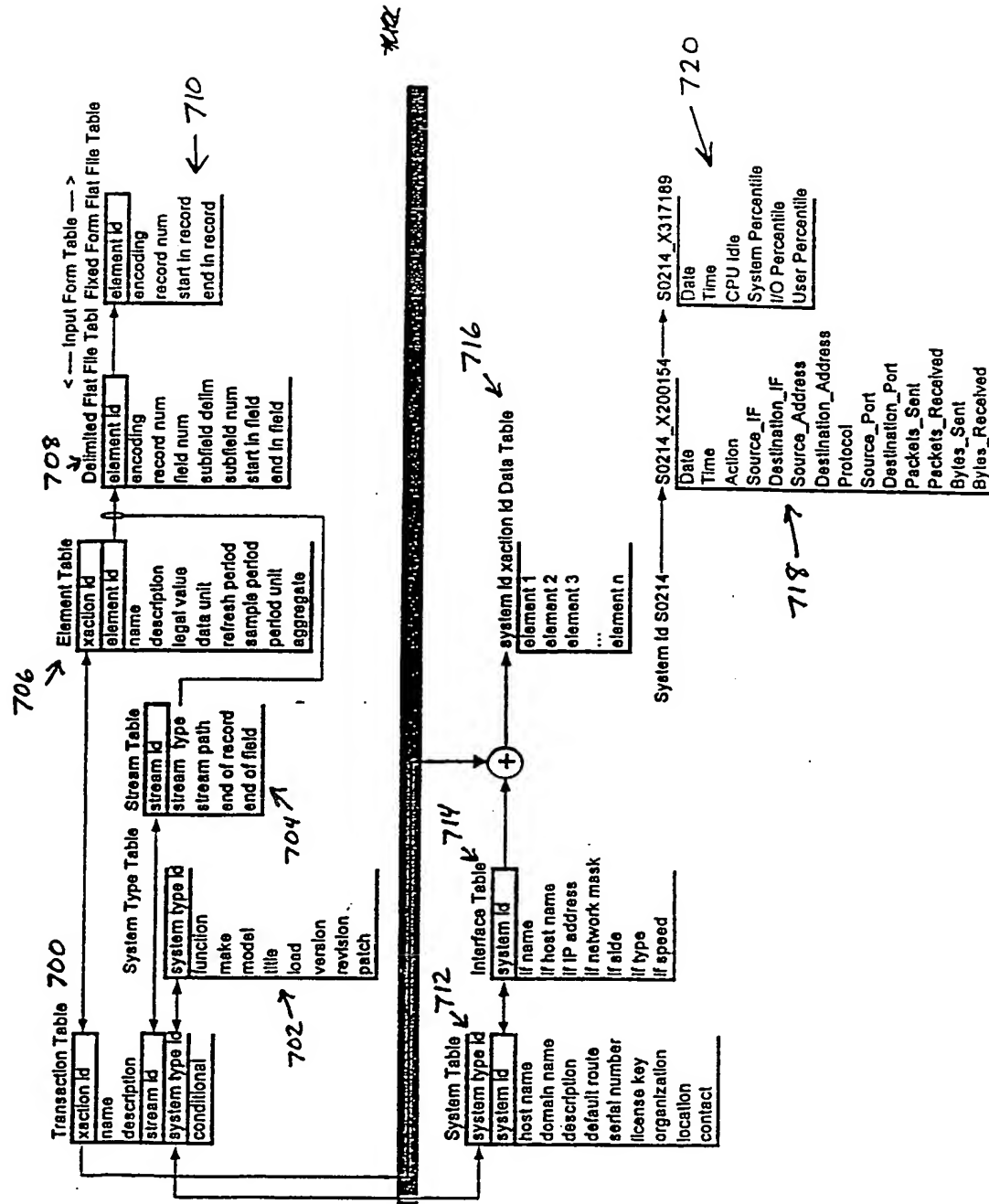Figure 9

1999/10/2709:00:00043004010023
1999/10/2709:10:00022003005010
1999/10/2709:20:00043004010023
1999/10/2709:30:00043004010023
1999/10/2709:40:00043004010023
1999/10/2709:50:00043004010023

Figure 10

S0214_X317189 Data Table

Date	Time	CPU Idle	System Percentile	I/O Percentile	User Percentile
1999/10/27	09:00:00	43	4	10	23
1999/10/27	09:10:00	22	3	5	10
1999/10/27	09:20:00	43	4	10	23
1999/10/27	09:30:00	43	4	10	23
1999/10/27	09:40:00	43	4	10	23
1999/10/27	09:50:00	43	4	10	23